U-M Common Windows Active Directory
Infrastructure Policies

(revision – 6/30/2004)

for more information on
the U-M Common Windows Active Directory Infrastructure and its support see
http://www.umich.edu/~lannos/windows/
All references to web documentation can be found within these pages.

Several Windows forests are currently in use at U of M for different purposes. This
document describes the Windows forest that is administered by the U-M Information
Technology Central Services (ITCS) in conjunction with the Windows IT-Commons
steewards. For brevity, references to the "U-M Forest" will refer to the U-M Common
Windows Active Directory Infrastructure.

The U-M forest is a university-wide collection of domains that are connected by trust
relationships, and share a common store of information, the Active Directory. Each
Windows AD domain maintains a separate namespace, yet resources can be shared
throughout the forest because of the trust relationships connecting the domains.

Given the distributed nature of the Active Directory (AD) and the potential for wide use
of the U-M Forest by the University of Michigan campus community, these policies were
developed to ensure that the forest provides a reliable resource to campus. The U-M
Forest is managed in a distributed fashion, therefore the rights and responsibilities in the
Forest break down into three areas: Enterprise Admins, Domain Admins and
Organizational Unit Admins. This policy will define those rights and responsibilities.

Forest Architecture Policies

- The Forest Root Domain, UMRoot (adsroot.itcs.umich.edu), anchors the U-M
  Forest.
- This domain contains user objects derived from and maintained by updates from
  the campus OpenLDAP directory. Privacy attributes in the OpenLDAP directory
  are maintained in Active Directory. Primary authentication of users in the
  UMRoot domain derived from OpenLDAP will be via passthrough authentication
  with the campus MIT KDC (Kerberos server). The MIT Kerberos password will
  be used and the Windows/AD password unknown.
- The UMRoot domain (adsroot.itcs.umich.edu) is maintained as a joinable campus
domain in which individual unit’s system administrators are given full rights to
administer delegated OUs for their unit. Units may create and maintain user accounts in their OUs that are independent of the centrally provided accounts as long as they follow naming standards for the forest.

- The number of Active Directory domains in the U-M forest will be carefully monitored. This is necessary to reduce complexity and manage network traffic, and to make better use of existing resources, keeping administrative costs down. New domains will be added as child domains of UMRoot. If you think your situation requires a dedicated domain please consult with the Windows Support Group.

- NTLM authentication will be allowed for a limited time. Due to the current reliance of Macintosh computers and legacy Windows OSes and applications, NTLM v.1 and v.2 authentication will be supported initially. As the technology advances, removing these dependencies, the level of authentication required will be strengthened.

- A PKI infrastructure is in place in the forest. Forest systems can receive certificates that allow SSL encryption at no additional cost. Public services should use commercial certificates such as Verisign.

- The members of the U-M Forest are committed to providing an up to date Windows/AD environment to campus. To that end, the goal is to adopt relevant new technology within 6 months of its release in the forest, particularly updates to technology current in use in the forest.

- The focus of the U-M Forest design and administration is to provide excellent service to Windows clients. The environment will not prevent access by non-Windows machines, and will allow and facilitate it whenever possible. However, if a change that will provide better service to Windows clients results in loss of functionality to non-Windows clients, the choice will favor the Windows clients.

### Enterprise Admin Rights and Responsibilities

The Information Technology Central Services (ITCS) LAN/NOS/Groupware Services (LNGS) team has been charged with the overall administration of the Active Directory Forest. ITCS-LNGS will provide trained Windows Administrators (MCSE level or equivalent) to maintain AD for the forest, provide central administration of the forest and provide support to Domain and Organizational Unit administrators on campus. This includes the following rights and responsibilities:

#### Maintain Active Directory

- **Maintain the forest root.** ITCS-LNGS delivers production Active Directory Services (AD) to the campus backbone on a 24x7 basis. To do so, it provides all server hardware, software, and networking necessary to maintain the AD forest root for the U-M forest. 24x365 monitoring and maintenance of file server hardware, software, and network up to the campus backbone is provided. In addition to simply maintaining these components, the AD service itself is secured, monitored and proactively maintained.
• Maintain Forest-wide Operations Masters: Schema Master and Domain Naming Master

• Communicate AD status. Department administrators are informed of AD status via the win2000@umich.edu listserv.

• Diagnose all reported AD problems.

• Provide backups for disaster recovery purposes. All LNGS-run Domain controllers are backed up nightly. These backups include the complete Active Directory contents for the Root and the Global Catalog of the Forest.

Provide Central Administration of the U-M Forest

• Provide updates to the User objects in the People OU from the U-M Online Directory (UMOD). ITCS-LNGS has populated the People OU of the UMRoot Domain with user objects from UMOD. New users and changes to privacy settings of existing users made to UMOD will be reflected in Active Directory immediately. Attribute changes to existing users made by 10:00pm on any business day will be reflected in the Active Directory by the 8:00am of the next business day.

• Provide a process to move user accounts into departmental OUs. Some circumstances require that the departmental admins be able to manage the users populated in AD from UMOD. ITCS LNGS will assist departments in determining this need and in providing a mechanism for moving accounts into departmental OUs, if this meets the need. The philosophy, architecture and process for this function are fully described in the Windows web pages.

• Manage Time. UMRoot Domain Controllers are set to use campus NTP servers to obtain time.

• Make schema modifications. Schema is the set of rules that govern the objects and attributes of objects in an AD forest. Upon the request of a department, the schema of the U-M Forest can be extended to allow for extensions to be made by Microsoft and third-party software. Before requesting that the schema be extended in the production forest, the requesting unit must test the change and its effects in the test forest. Once the change has been tested and an official request has been made, ITCS-LNGS will send out a message to win2000@umich.edu to give departmental admins the opportunity to express any concerns they have about the extension. If no issues surface within two weeks, the schema will be extended at the forest root, allowing departmental administrators to install the software making use of those extensions. Note: schema extensions will NOT be made for beta version products or pre-release product updates.

• Maintain security at the forest root. Access to the forest root is granted only to trusted and trained members of the ITCS-LNGS team for forest administration only. All root admins use normal accounts for non-AD administrative activities.
• **Maintain site-level security policy.** The Active Directory architecture provides the ability to apply group policy and security to all systems within a site. By default, no policies will be made to the forest default site. Any changes will be presented to the Windows Core Working Group and the Windows community and before implementation.

• **Maintain Root Certificate Authority (CA) and Issuing CA.** Create and maintain the Root CA (used to establish the forest root authority) plus an issuing CA (used for creating certificates), which can be used to create Public Key Infrastructure key pairs throughout the tree.

• **Maintain Root Exchange Servers.** Create and maintain the Root Exchange servers so that departments may add their own Exchange servers to the forest. A central Global Address list is maintained for the entire forest. Manage the shared Public Folder structure.

• **Manage Root-level DNS.** Manage forward zones for Root Domain Controllers. ITCS will also manage forward zones for departments or domains if they so choose.

• **Maintain test forest for internal and campus testing.** ITCS-LNGS provides a Windows/AD test environment that mimics the production environment so that services can be tested and questions answered before introducing them into the production environment. Any department can participate in the test tree in a manner appropriate to the way that they will participate in the U-M Forest. Testing in the test forest is required before departments can join the production tree as a separate Domain. Testing may also be required before new services or applications are introduced into the production forest.

### Support all Department Admins

• **Windows Administrators Group.** ITCS-LNGS sponsors this user group on campus, including an e-mail list at win2000@umich.edu.

• **Windows Core Working Group.** ITCS-LNGS participates in this group to share information and to obtain input from campus participants on technical direction and planning issues for campus, including critical security issues. Membership in this group is limited to departments and individuals who actively participate in and contribute to this effort. Members of the Windows Core Workg Group are expected to have a high level of expertise with Windows technology. Send email to wincwg@umich.edu for membership information.

• **Microsoft Custom Enterprise Agreement.** Departments of the University of Michigan have collectively purchased licenses for faculty and staff for a select set of Microsoft products. For more information about the MCEA, see http://www.itd.umich.edu/microsoft/MicroDept.html. This agreement is managed by ITCS Licenses (licenses.itd@umich.edu).

• **Recommend patches and upgrades.** Due to the critical nature of many Windows patches, ITCS-LNGS does not recommend waiting for any central resource for advice.
on applying patches. In general, critical security patches should be applied within 24-48 hours of their release. Non-critical patches and larger service packs can tolerate a longer validation period, and units should do testing against applications and services they provide to determine the suitability of the updates. Microsoft patches in the forest environment have not been shown to affect other members of the environment and so application of those patches is an individual decision, with the exception of critical security patches which should be applied immediately.

- **Problem resolution.** ITCS-LNGS acts as second-line support on U-M Forest infrastructure issues to department admins.

**Maintain support for Departmental Admins**

Departments can join the U-M Forest in one of two ways: UMROOT domain OU or Department-sponsored Domain.

- **UMROOT Domain OU** provides services to users within their OU, other OUs and domains in the forest, and users in the People OU. All Active Directory services responsibilities are handled by ITCS.

- **Department-sponsored Domain** is a separate domain that manages all services and users within the domain, including Active Directory Services. They provide services to users in their own and other domains in the forest, including users in the People OU.

**Support Campus Tree OU Admins**

- **Provide DNS services** for the UMROOT Domain

- **Maintain the Active Directory for the UMROOT Domain**, including Global Catalog servers and all Domain-specific Operations Masters (RID Master, PDC Emulator and Infrastructure Master)

- **Create Organizational Units for departments.** Organizational Units are created as sub-containers within the Organizations. Within that OU, an admin user object is created and made a member of an OU Admin security group, with full rights to administer objects within that OU.

- **Otherwise maintain a hands-off policy towards OU administration.** Only if necessary in an emergency will Enterprise Admin rights be used to take action in a Department-sponsored OU. If such action is necessary, the local OU admin will be notified and, if possible, consulted in a timely manner.

**Support Domain Admins**

- **Review requests for Department-sponsored Domains** and grant or deny request (see Department-sponsored Domain Admins Rights and Responsibilities below).
These requests will be reviewed in conjunction with the IT-Commons Stewards of the U-M Common Windows Environment.

- **Provide a consultation** with departmental admins to review plans before admission to the U-M Forest as a Domain.

- **Be available to authenticate the DCPROMO process**, as required for the new Domain to join the forest.

- **Ensure that these policies are being followed** and communicate any issues to the local administrator(s) for resolution.

- **Otherwise maintain a hands-off policy towards Domain administration.** Only if necessary in an emergency will Enterprise Admin rights be used to take action in a Department-sponsored Domain. If such action is necessary, the local domain admin will be notified and, if possible, consulted in a timely manner.

**Departmental Admin Rights and Responsibilities**

Departments must designate one or more System Administrators to provide system administration for departmental servers. Overall administration of the U-M Forest is a joint venture between department administrators and ITCS-LNGS Enterprise Administrators. This includes the following rights and responsibilities.

- **Manage local services.** Departments have full autonomy in managing their local servers and services. This includes installing and removing servers, creating shares, creating users and groups, placing local users (see next item) and People OU users into groups assigning rights and permissions and managing printing resources. In general, hardware and software updates can be implemented at the department’s discretion. However, there are times that departments will be required to update software to maintain the integrity of the U-M Forest.

- **Create and manage local user accounts.** Local user accounts may be created within UMROOT Domain OUs and Department-sponsored Domains. These accounts will not have UM MIT Kerberos interoperability, but will be fully manageable by departmental admins. Note that user accounts created within UMROOT Domain OUs must adhere to naming standards for the forest to avoid namespace collisions with current or potential Kerberos identities.

- **Create and manage Organizational Units.** Departments can sub-divide their own containers into Organizational Units to facilitate their local management. This can be done at the department’s discretion and according to the department’s design. ITCS-LNGS maintains the top-level organization only.

- **Provide contact information.** Each container must contain contact information for the department to facilitate contacting departmental admins. Use the Managed by property of your Organizational Unit or Domain to provide the name, e-mail address, phone number, pager number and location of the administrator(s) responsible for that container.
• **Maintain Security.** Each department is responsible for maintaining their own environment securely.

• **Use recommended naming standards as documented on the Windows web pages.**

**Additional Responsibilities of Domain Admins**

• **Meet requirements as outlined in the Domain Policy.** Because the number of Windows domains in the forest impacts Active Directory replication, ITCS LNGS must take an active role in monitoring the number of domains. In addition, it is critical that they be properly monitored and maintained. To ensure that this is done, a more detailed Domain Policy must be agreed to by units running their own domains. Please see Addendum A for this policy.

• **Maintain Active Directory for the Domain,** including Global Catalog servers and all Domain-specific Operations Masters (RID Master, PDC Emulator and Infrastructure Master).

• **Keep servers available.** For Active Directory synchronization to function correctly, all Domain Controllers in the tree must be available at all times. If it is necessary to down your DC for more than a few hours, you must contact ITCS-LNGS. Servers brought down permanently must be properly removed from AD. If you don’t know how to do this, contact ITCS-LNGS before downing the server.

• **Follow proper procedures when adding or removing Domain Controllers.** Submit “Domain Controller Information Forms” when changes are made.

• **Maintain security.** Regularly review usage for “Everyone”, provide access on a ‘need to know’ basis, scan all domain resources annually, and use monitoring and auditing where needed.

• **Work collectively with other Domain Admins.** Issues that could apply to others should be discussed and shared. Doing so helps to maintain a coherent infrastructure and to allow for economies of scale through campus-wide purchases and support. Use [Win2000@umich.edu](mailto:Win2000@umich.edu) to communicate issues of importance to other campus administrators.

**Contact Information**

For more information on how these policies are implemented and for technical information about deploying Windows/AD on campus, including procedures referred to in this document, see [http://www.umich.edu/~lannos/windows](http://www.umich.edu/~lannos/windows).

If a department needs to contact ITCS-LNGS for routine administrative matters, they should send e-mail to [w2k.support@umich.edu](mailto:w2k.support@umich.edu). **This e-mail is monitored by the ITCS-LNGS team responsible for Windows/AD and will be answered promptly.** If more immediate support is needed, the department may contact one of the members of the group, discovered by querying [http://directory.umich.edu](http://directory.umich.edu) for the members of the above e-mail group.
The system administrators of Department-sponsored Domains perform management of departmental OUs under those domains. Administrators of departments within these domains should contact the appropriate IT department for help with Windows and Active Directory issues. See the Windows web pages for this information.

The ITCS Windows/AD team performs routine maintenance and upgrades on the root servers during maintenance windows scheduled in very early morning or late at night with the intent of minimizing impact on users. These outages will be scheduled in advance and sent to the joinable email list, umroot.notify@umich.edu. The maintenance window will be published in the Windows web pages in the future.

**Addendum A: U-M Forest Domain Policy**

**Introduction**

Information Technology Central Services (ITCS) actively monitors the proliferation of separate domains in the U-M Forest and encourages as many units as possible to join the infrastructure as OUs within the campus forest. The reasons for wanting to limit the domain proliferation are technical, not political or arbitrary. Each additional domain increases Active Directory replication traffic across U-M campus networks. This consumes bandwidth and creates an increasingly complex environment.

A long term goal for the forest is to maintain a single account domain. Entries from the enterprise campus directory are automatically added to the Active Directory to populate this single account domain. Multiple account domains causes confusion for users.

**Domain versus Organizational Unit**

Departments wish to be able to manage their own resources in the Windows/AD environment. LAN/NOS/Groupware Services is providing an Active Directory forest for the campus community. Within the campus environment, a unit may join as a delegated Organizational Unit (OU) or as a separate Domain. There is considerable difference in commitment of resources between joining the campus forest as an OU or a Domain. To join the campus environment as an OU, one only needs to provide servers for the resources they plan to provide for their customers. To join as a Domain, at least 2 servers must be dedicated as Domain Controllers (DCs). These DCs are critical to the functioning of the entire forest, and need to be carefully tended. For information on the functional differences between joining the forest as a separate OU versus a Domain, please refer to the following table.

<table>
<thead>
<tr>
<th>Rights/advantages</th>
<th>OU</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set password policies</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Assign group policy</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Manage resources</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Provide Exchange mailboxes for users</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change users’ passwords</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Provide file space for users</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Create departmental user accounts non uniqnames</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Create departmental user accounts with uniqname</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Responsibilities/issues**

<table>
<thead>
<tr>
<th>OU</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Domain Controllers</td>
<td>✓</td>
</tr>
<tr>
<td>Meet requirements outlined below</td>
<td>✓</td>
</tr>
<tr>
<td>Participate in campus Windows listserv</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Requirements for Joining the U-M Forest as a Domain**

In order to join the U-M Forest as a Domain, the department head or dean must sign an agreement committing to proper use and maintenance of the domain as outlined in this document, including:

- Request at most one Windows Domain per organization, as defined by the Standard Practice Guide for DNS domains in section 601.15-1

- Support at least two full time system administrators (primary and backup), Windows certified or with at least 2 years Windows/AD administration experience.

- Require participation of system administrator(s) in the campus Windows administrators group and the Windows Core Working Group, to facilitate discussions and decisions about global infrastructure.

- Provide contact information for Windows system administrators, including business hours and after hours accessibility.

- Dedicate at least two (2) Windows servers to act as Domain Controllers and only Domain Controllers for their Domain. These servers must be running on server-class hardware with fault-tolerant disk arrays, UPS power systems, maintained and updated (including hardware upgrades) as necessary to provide good quality replication on campus and must be located in a physically secure area.

The department system administrators must agree to follow the policies outlined in this document and to:

- Test planned implementation in the test forest before joining the production forest.
Consult with LNGS Windows team (in conjunction with the IT-Commons Windows stewards) for design and implementation approval before joining the forest.

Submit a “Domain Information Form” to LNGS. Submit new forms for subsequent changes. See attached form. Enter contact information in the “Managed By” tab of the domain properties in Active Directory.

Submit a “Domain Controller Information Form” to LNGS for each new or changed server. See attached form.

Notify wincwg@umich.edu at least 2 weeks prior to adding or removing a Domain Controller or Global Catalog in the domain.

(Note on Global Catalog Servers: Placement and number of Global Catalog servers is probably the most significant contributor to the replication issues caused by multiple domains. Changes made to attributes replicated by GCs are sent to every GC on campus. Access to a GC is critical because without it login cannot occur)

Run only those services on Domain Controllers that are necessary for the functioning of the domain, for example, Kerberos, LDAP, DNS/DHCP, Dfs.

Do not run services that increase exposure to security risks on Domain Controllers, for example, IIS, Exchange, Certificate Services, WINS, Proxy Services, FTP, SMTP, telnet, Simple TCP/IP services.

Employ whatever monitoring or other resources are necessary to keep the DCs healthy and available at all times. Ping monitoring is a minimum.

Give advance notice of at least 2 days to w2k.support@umich.edu if it is known that a DC will be down for more than a few hours

Notify w2k.support@umich.edu if a DC is unavailable because of problems

Apply updates (hot fixes, service packs) to Domain Controller servers upon request from central LNGS Windows/AD team in a timely manner

Cooperate with the LNGS Windows/AD team to correct problems with replication

Leave the Enterprise Administrator group in the Domain Administrators Group to allow for central access to all domain controllers.
• Maintain a presence in the test forest, using it to test new implementations, patches and software before deploying in production and to test the effects of changes to the forest itself.

• Limit trusts connecting Windows domains to NT4 domains to a very short period of time (1 day to 1 week), using them only for domain migrations.
Domain Information Form

To initiate the process of join the U-M W2k forest as a domain, the U-M campus organization should fill out the following form, cut-and-paste the form into an email message, and send the message to W2kSupport@umich.edu. If you have more, or fewer subnets, DNS servers, etc. than the form displays, just add or delete as needed.

**************************************************************
FORM: CreateDomain
**************************************************************
Organization:
Street Address 1:
Street Address 2:
City:
State:
Zip Code:
Telephone1:
Telephone2:

Full Domain Name:
NetBIOS Domain Name:
Native Mode:
External Trusts:
DNS Server 1:
DNS Server 2:
WINS Server:
GC Server:
Subnet 1:
Subnet Mask 1:
Subnet 2:
Subnet Mask 2:
Other:
Other:

Administrator1
Full Name:
U-M uniqname:
Email address:
Phone:
Pager:

Administrator2
Full Name:
U-M uniqname:
Email address:
Phone:
Pager:

Administrator3
Full Name:
U-M uniqname:
Email address:
Phone:
Pager:

**************************************************************
END_FORM: CreateDomain
**************************************************************

Evaluation notes were added to the output document. To get rid of these notes, please order your copy of ePrint IV now.
Domain Controller Information Form

To initiate the process of adding or changing domain controllers in the domain, the U-M campus organization should fill out the following form, cut-and-paste the form into an email message, and send the message to W2kSupport@umich.edu. If you have other services or information than the form displays, just add or delete as needed.

************************
FORM: CreateDomainController
************************

Organization:
Fill in address of server location
Street Address 1:
Street Address 2:
City:
State:
Zip Code:
Site Administrator:
Telephone1:
Telephone2:

Full Domain Name:
NetBIOS Domain Name:
Server Name:
Server IP:
Win2000 Site:
Connectivity to Central Campus:

Services – Type YES for all that apply
DNS Primary:
DNS Secondary:
GC:
DHCP:
DFS Root:
Other:

FSMO Roles – Type YES for all that apply
PDC:
RID:
Infrastructure:

************************
END_FORM: CreateDomainController
************************